Table of Contents

Tux2010 setup notes.

```
            Time-stamp: <2010-12-14 23:19:37>
            --------------------------------
            file tux2010_installation_notes.txt

file created 2010/12/14

Notes for installation of Debian 5.06 (Lenny) on new hardware for
OCLUG machine "tux2010".

Machine currently resides at the home of Richard Guy Briggs in Ottawa Ont.

2010/11/26
- The first installation attempt involved some experimentation to
  determine the correct procedure for configuring the software raid
  with LVM.
  Although the DVD installation completed, network problems prevented
  software updates and further configuration.
  It was decided that the installation would be restarted at a later
  date to allow accurate documentation of the exact procedure.
- Items learned:
  - Although the DVD contains all the files needed for the
    installation, it accesses the net if one is present.
    This may be an installation bug but since a slow network will
    cause an installation time estimate of over 24 hours, it's
    difficult to document what s/w is being installed.
    This problem isn't present when installing from DVD without the
    network connected.
    Therefore: Disconnect the network, install the Debian OS and
    configure the network later.
  - When removing partitions from an existing LVM installation, it
    wants to "clear" the partitions.  This can take hours to cleanly
    remove partitions from a disk that we only wish to "trash", ie:
    use as a new blank disk.
    Therefore: Use the fdisk command to quickly destroy disk partitions.


2010/12/02
- Second installation attempt.  This one was successful.
  Although the network issues have been resolved by replacing the disk
  on a firewall machine, the initial installation is being done with
  the network disconnected.

- Booted Debian 5.06 DVD: started installation, but found we had trouble
resetting the disk partitions. Therefore opened a shell and ran
fdisk /dev/sda
```

```
and D(eleted partition)   1
W(rite)

fdisk /dev/sdb
and D(eleted partition)   1
W(rite)

Rebooted to ensure this was registered.
When we tried an install, we discovered the machine was attempting to
use the network, so the cable was unplugged and the installation restarted.

Restarted installation:
    English, Canada, American English
    Machine name: tux2010
(No network available, so no domain yet configured.)
Note: If a machine has 2 hardware disks, the following procedure will
    configure software raid and then use LVM (the Logical Volume Manager).
Partitioning:
    Chose FREE SPACE on first disk and used all space with
        Create Partition
            Use as physical volume for RAID
    Same on second disk
    Configure s/w RAID
        Keep partitions and configure RAID
        Create MD device
        RAID1,   2 devices
        No. of spares 0
        Select BOTH devices
        Finish

    Configure LVM
        Keep layout (Y)
        Deleted all Logical Volumes (seems to remember them)
        Deleted volume group
        Create Volume Group        tx
        Select /dev/md0
        Create logical volumes             intended use
      name  size            mount point
            t1     250M         /boot
            t2    10G           /
            t3    8G            swap
            t4    50G           /var
            t5    10G           /tmp
            t6    20G           /usr
            t7    20G           /home
        Select each LV in turn, and choose "Use as ext3" for all but t3
            which is "Use as swap"
            For all but t3, choose "Format this partition" and select
```

```
            the appropriate mount point as given above
        Finish and write partition table. (Yes)

    Enter root pw (_______),
    Create user named "installer", username "install", same pw as root.
    Scan another CD/DVD:     No
    Choose:
    s/w installation
    [[:x]] desktop environment
    [[:x]] standard system
    Note: Choosing the desktop environment installs more s/w than
          desired but is but is easier than manually selecting all the
      packages we DO need.
    Note: Lilo was installed by default.  Grub wasn't offered (or needed).

    When done, Lilo target        /dev/md0
    Large memory option for Lilo        Yes
    Write lilo /sbin/lilo
    Reboot.

    Hostname: tux2010

Network configuration:
    Log in as install.
    Menu: System / Administration / Network
          (This runs the command /usr/bin/network-admin.)
    On the Connections tab
    Choose Wired connection  (eth0)
    static
    [ ] Enable roaming mode   (ie: Don't select it.)
    Configuration:   Static IP address
    IP address:      204.224.221.7
    Subnet mask:     255.255.255.224
    Gateway address: 204.224.221.1

    On the DNS tab:
    DNS servers select add
    DNS server:      204.224.221.2

    This results in:
    tux2010% /sbin/ifconfig
    eth0      Link encap:Ethernet  HWaddr 00:12:3f:d2:a5:cc
          inet addr:204.225.221.7  Bcast:204.225.221.31  Mask:255.255.255.224
          inet6 addr: fe80::212:3fff:fed2:a5cc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:215258 errors:0 dropped:0 overruns:0 frame:0
          TX packets:68354 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
```

```
          RX bytes:25921523 (24.7 MiB)  TX bytes:11935741 (11.3 MiB)

    lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1429 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1429 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2166668 (2.0 MiB)  TX bytes:2166668 (2.0 MiB)

As root (su):
    run command "su", enter root password then run the following:
    /etc/init.d/networking restart
    visudo
        add    install
    The following line is added to file /etc/sudoers
    install ALL=(ALL) ALL

Updates
    Menu: System / Administration / Synaptic package manager
    Settings
        Choose debian.yorku.ca as repository server
        Choose only main collection for now.
    From the command line, run:
    apt-get update
    apt-get upgrade
    apt-get install rsync ssh

After updates, disk usage is:
    tux2010% df -h
    Filesystem            Size  Used Avail Use% Mounted on
    /dev/mapper/tx-t2     9.2G  231M  8.5G   3% /
    tmpfs                1014M     0 1014M   0% /lib/init/rw
    udev                   10M  736K  9.3M   8% /dev
    tmpfs                1014M     0 1014M   0% /dev/shm
    /dev/mapper/tx-t1     229M   23M  194M  11% /boot
    /dev/mapper/tx-t7      19G  174M   18G   1% /home
    /dev/mapper/tx-t5     9.2G  150M  8.6G   2% /tmp
    /dev/mapper/tx-t6      19G  2.1G   16G  12% /usr
    /dev/mapper/tx-t4      46G  449M   44G   2% /var

  Note: For old tux:
    tux% df -h
    Filesystem            Size  Used Avail Use% Mounted on
    /dev/sda3             9.4G  7.8G  1.2G  88% /
    tmpfs                 379M     0  379M   0% /lib/init/rw
    udev                   10M   88K   10M   1% /dev
```

```
    tmpfs                  379M     0  379M   0% /dev/shm
    /dev/mapper/TuxGroup-TuxHome
              5.0G  1.1G  3.6G  24% /home

Services:
    Menu: System / Administration / Services
        Check OFF: exim4 (mail agent)
        Check OFF: rsync remote backup server
        Check ON: ssh

Adding user accounts for: roland, nashjc
  Note: The following useradd command required the home directory to
  be manually created and ownership changed.  The correct commands are
  described in the 2010/12/06 entry in this file.
  The incorrect commands are documented here for the sake of accuracy.

useradd -c "Roland Renaud"  -s /bin/bash -d /home/roland -u 1020 -g users
roland

useradd -c "John Nash" -s /bin/bash -d /home/nashjc -u 1021 -g users nashjc

tux2010% grep roland /etc/passwd
    roland:x:1020:100:Roland Renaud:/home/roland:/bin/bash
tux2010% grep nashjc /etc/passwd
    nashjc:x:1021:100:John Nash:/home/nashjc:/bin/bash

root@tux2010:/home# mkdir nashjc
root@tux2010:/home# chown nashjc.users nashjc

    Later found nashjc had ownership roland:users. And since tux2keys dir
    on USB key was on fat filesystem, the permissions were 755, not
    700 for directory and 600 for files in .ssh

- tux2 visible to the world and accepts passwd login.

Making ssh key for user "install".

  Note: This was created on Roland's laptop running Ubuntu Lucid.
rjrlap3% ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/usr/home/roland/.ssh/id_rsa):
./id_rsa_tux2
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in ./id_rsa_tux2.
Your public key has been saved in ./id_rsa_tux2.pub.
The key fingerprint is:
32:1e:e7:7c:4a:1f:63:79:18:94:68:65:41:a8:8f:62 roland@rjrlap3
```

```
The key's randomart image is:
+--[ RSA 2048]----+
|         o=.     |
|        .+ .     |
|       .o o      |
|      .. .       |
|      +oS .      |
|    E..B.  +     |
|   . .. + B .    |
|       . = +     |
|        . .      |
+-----------------+

  At this point these were made without a passphrase, which JN had used to
allow
  for automatic unattended backups from his own server. However, there would
be
  better security with a passphrase.

rjrlap3% rsync -av *pub install@tux2:.ssh

root@tux2010:/home/install/.ssh# cat id_rsa_tux2.pub >> authorized_keys

Disable password login:
  cp -p sshd_config sshd_config.orig
  edit sshd_config  to configure
      PasswordAuthentication no
Note: Remote login to machine tux2010 is now only possible using ssh
      with keys.  Passwords are disabled.



2010/12/06
new Tux (tux2010) - configuration continued.

Adding user accounts for current OCLUG board of directors and user "rgb".
    New tux (204.225.221.7 tux2010)
    Old tux (204.225.221.10 tux)

Information obtained from old tux:
 - username, user id from file /etc/passwd
 - encrypted passwords from file /etc/shadow
 - ssh keys from file /home/username/.ssh/authorized_keys

Once users have configured ssh-agent on their home machine, they
should be able to login to new tux with the command "ssh -AY tux2010"
(or "ssh -AY 204.225.221.7") as with old tux.

They have the same userid, passwd, sudo privs and ssh keys as before.
```

```
For consistency, everyone is now in the "users" group (100).
We'll determine later if it's worth the trouble to maintain other
group lists such as "board" or if some users should have their own
group.
(Apparently, group names are automatically generated by some
account adding s/w.)

Home directory configs weren't copied.
To copy it, users can log into tux and run something like this:
    rsync -av $USER tux2010:
(Old tux has tux2010 in its hosts file.)

How it was done.  Note: Passwords modified for this document.
The real encrypted passwords can be obtained from the file /etc/shadow.
Updating the old passwd might be a good idea.
Even re-entering the old password on the new machine will cause the
encryption in /etc/shadow will be different from old tux.

Note: To remove a user and their files, run this command as root.
        userdel -r username    (eg: userdel -r roland)

Therefore, the following commands were used.
Information for users roland and nashjc are here for reference only.


useradd -c "Roland Renaud" -s /bin/bash -m -u 1020 -g users -p '$1$CYf/'
roland

useradd -c "John Nash" -s /bin/bash -m -u 1021 -g users -p '$1$mc/0' nashjc

useradd -c "Lisa Lovchik" -s /bin/bash -m -u 1010 -g users -p '$1aU.' exexpat

useradd -s /bin/bash -m -g users -c "Eric Brackenbury" -u 2007 -p '$1$G0'
ericb

useradd -s /bin/bash -m -g users -c "John Sebastien Taylor" -u 2008 -p '$1C1'
johnsebastientaylor

useradd -s /bin/bash -m -g users -c "Mike Kenzie" -u 2009 -p '$1$a1' kenziem

useradd -s /bin/bash -m -g users -c "RichardGuyBriggs" -u 1002 -p '$1z' rgb

Added to /etc/sudoers
    roland  ALL=(ALL) ALL
    nashjc  ALL=(ALL) ALL
    exexpat ALL=(ALL) ALL
    ericb   ALL=(ALL) ALL
    kenziem ALL=(ALL) ALL
```

```
    rgb     ALL=(ALL) ALL
    johnsebastientaylor    ALL=(ALL) ALL

Therefore, the file /etc/passwd contains the following lines:
    roland:x:1020:100:Roland Renaud:/home/roland:/bin/bash
    nashjc:x:1021:100:John Nash:/home/nashjc:/bin/bash
    ericb:x:2007:100:Eric Brackenbury:/home/ericb:/bin/bash
    johnsebastientaylor:x:2008:100:John Sebastien
Taylor:/home/johnsebastientaylor:/bin/bash
    kenziem:x:2009:100:Mike Kenzie:/home/kenziem:/bin/bash
    rgb:x:1002:100:RichardGuyBriggs:/home/rgb:/bin/bash
    exexpat:x:1010:100:Lisa Lovchik:/home/exexpat:/bin/bash


Installing ssh keys for each user:
    cd /home/username
    mkdir .ssh
    copy key from old tux
    chown -R username.users .

Some script scraps.
This was run on old tux.
cd /home
for f in ericb exexpat johnsebastientaylor kenziem
do
    echo ---- $f ----
    tar rvf /home/roland/k2.tar $f/.ssh/authorized_keys
done



    root@tux% sh xx
    ---- ericb ----
    ericb/.ssh/authorized_keys
    ---- exexpat ----
    exexpat/.ssh/authorized_keys
    ---- johnsebastientaylor ----
    tar: johnsebastientaylor/.ssh/authorized_keys: Cannot stat: No such file
or directory
    tar: Error exit delayed from previous errors
    ---- kenziem ----
    kenziem/.ssh/authorized_keys

    root@tux% chown roland.users ~/k2.tar


Back to tux2010:
    root@tux2010% cd /home
    root@tux2010% tar tvf ~roland/k2.tar
```

```
    -rw-r--r-- ericb/ericb     391 2010-09-10 21:49 ericb/.ssh/authorized_keys
    -rw-r--r-- exexpat/exexpat 398 2010-10-05 15:03
exexpat/.ssh/authorized_keys
    -rw-r--r-- kenziem/kenziem 400 2010-08-20 00:33
kenziem/.ssh/authorized_keys
    root@tux2010% tar xvf ~roland/k2.tar
    ericb/.ssh/authorized_keys
    exexpat/.ssh/authorized_keys
    kenziem/.ssh/authorized_keys

Hmmm, root ended up owning the .ssh directories.  Fixing:
    cd /home
    chown -R ericb.users ericb
    chown -R exexpat.users exexpat
    chown -R kenziem.users kenziem

Notes:
  - RGB has authorized_keys2 instead of authorized_keys.
    I copied this manually.
    He also has another key there.  I'll let him take care of that.
  - JST will have to send us his public key if he wants to login.

Note:  Internet attacks start 65 minutes after machine is connected to net.
Good thing we only accept ssh keys.
Information from /var/log/auth.log.
Dec  2 11:38:04  - Machine tux2010 was alive
Dec  2 13:09:00  - machine connected to the network.
Dec  2 13:12:31  - added account for user roland
Dec  2 13:29:47  - added account for user nashjc
Dec  2 14:14:11 tux2010 sshd[[:9825]]: Address 217.174.249.24 maps to
       mail.compushopdirect.com, but this does not map back to the address -
       POSSIBLE BREAK-IN ATTEMPT!
```